CLAIM LISTING

Amendments to the claims are reflected in the following listing, which replaces any and all prior versions and listings of claims in the present application:

Amendments to the Claims:

1. (Currently Amended) A smartcard transaction system configured with a biometric security device ~~system~~, said system comprising:

a smartcard configured to communicate with a reader,; ~~a~~ wherein said reader configured to communicate with said system;

an integrated circuit device disposed within said smartcard and configured to communicate with said reader, said integrated circuit device comprising a common application and a second application, said second application being configured to store travel-related information associated with a cardholder;

said second application comprising a common file structure and a partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to file in said common file structure;

a smellprint sensor configured to detect a proffered smellprint sample, said smellprint sensor configured to communicate with said system; and,

a device configured to verify said proffered smellprint sample to facilitate a transaction based on at least one of said partner file structure and said common file structure.

2. (Original) The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

3. (Currently Amended) The smartcard transaction system of claim 1, wherein said partner file structure enables said first partnering organization to

program said smartcard as a room key ~~smellprint sensor is configured to facilitate a finite number of scans~~.

4. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor is configured to log at least one of a detected smellprint sample, processed smellprint sample and stored smellprint sample.

5. (Original) The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered smellprint samples, proffered and registered user information, terrorist information, and criminal information.

6. (Original) The smartcard transaction system of claim 5, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

7. (Original) The smartcard transaction system of claim 6, wherein said remote database is configured to be operated by an authorized sample receiver.

8. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor device is configured with at least one of an electronic sensor, chemical sensor, gas chromatograph, spectrometer, conductivity sensor and piezoelectric sensor.

9. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor is configured to detect and verify smellprint characteristics using at least one of statistical, ANN and neuromorphic techniques.

10. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor is configured to detect and verify smellprint characteristics including molecular structures, chemical compounds, temperature, mass differences, pressure, force and odorants.

11. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor device is configured to detect false odorants, man-made smells, abnormal odorants and body heat.

12. (Original) The smartcard transaction system of claim 1, further including a device configured to compare a proffered smellprint sample with a stored smellprint sample.

13. (Original) The smartcard transaction system of claim 12, wherein said device configured to compare a smellprint sample is at least one of a third-party security vendor device and local CPU.

14. (Original) The smartcard transaction system of claim 12, wherein a stored smellprint sample comprises a registered smellprint sample.

15. (Original) The smartcard transaction system of claim 14, wherein said registered smellprint sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

16. (Original) The smartcard transaction system of claim 15, wherein different registered smellprint samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

17. (Original) The smartcard transaction system of claim 15, wherein a smellprint sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a smellprint sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

18. (Original) The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered smellprint sample.

19. (Original) The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered smellprint sample.

20. (Currently Amended) The smartcard transaction system of claim 1, wherein said first partner file structure includes card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel. ~~said sensor is configured to provide a notification upon detection of a sample~~.

21. (Currently Amended) The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least ~~one~~ two of access to a product, activation of a device, a financial transaction, and a non-financial transaction.

22. (Original) The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

23. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system comprising: proffering a smellprint to a smellprint sensor communicating with said system to initiate verification of a smellprint sample for facilitating authorization of a transaction based on at least one of a partner file structure and a common file structure stored on a smartcard having an integrated circuit device comprising a common application and a second application, said second application being configured to store travel-related information associated with a cardholder;

said second application comprising said common file structure and said partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to a file in said common file structure.

24. (Original) The method for of claim 23, further comprising registering at least one smellprint sample with an authorized sample receiver.

25. (Original) The method of claim 24, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a smellprint to said authorized sample receiver, processing said smellprint to obtain a smellprint sample, associating said smellprint sample with user information, verifying said smellprint sample, and storing said smellprint sample upon verification.

26. (Original) The method of claim 23, wherein said step of proffering includes proffering a smellprint to at least one of an electronic sensor, chemical sensor, gas chromatograph, spectrometer, conductivity sensor and piezoelectric sensor.

27. (Original) The method of claim 23, wherein said step of proffering further includes proffering a smellprint to a smellprint sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said smellprint sample.

28. (Original) The method of claim 23, wherein said step of proffering a smellprint to a smellprint sensor communicating with said system to initiate verification further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

29. (Original) The method of claim 23, wherein said step of proffering a smellprint to a smellprint sensor communicating with said system to initiate verification further includes comparing a proffered smellprint sample with a stored smellprint sample.

30. (Original) The method of claim 29, wherein said step of comparing includes comparing a proffered smellprint sample to a stored smellprint sample by using at least one of a third-party security vendor device and local CPU.

31. (Original) The method of claim 29, wherein said step of comparing includes comparing smellprint characteristics using at least one of statistical, ANN and neuromorphic techniques.

32. (Original) The method of claim 23, wherein said step of proffering a smellprint to a smellprint sensor communicating with said system further comprises using said smellprint sensor to detect at least one of false odorants, man-made smells, abnormal odorants and body heat.

33. (Original) The method of claim 23, wherein said step of proffering a smellprint to a smellprint sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered smellprint sample.

34. (Original) The method of claim 23, wherein said step of proffering a smellprint to a smellprint sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure.

35. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system comprising:

detecting a proffered smellprint sample at a sensor communicating with said system ~~to obtain a proffered smellprint sample~~;

verifying the proffered smellprint sample; ~~and~~

authorizing a transaction to proceed upon verification of the proffered smellprint sample; and

accessing at least one of a partner file structure and a common file structure stored on a smartcard having an integrated circuit device comprising a common application and a second application, said second application being configured to store travel-related information associated with a cardholder;

said second application comprising said common file structure and said partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to a file in said common file structure.

36. (Original) The method of claim 35, wherein said step of detecting further includes detecting a proffered smellprint at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

37. (Original) The method of claim 35, wherein said step of detecting a proffered smellprint includes detecting a proffered smellprint at least one of an electronic sensor, chemical sensor, gas chromatograph, spectrometer, conductivity sensor and piezoelectric sensor.

38. (Original) The method of claim 35, further comprising updating card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel is said first partner file structure ~~wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered smellprint sample~~.

39. (Original) The method of claim 35, further comprising writing to at least one of said partner file structure and said common file structure to program said smartcard as a room key ~~wherein said step of detecting further includes receiving a finite number of proffered smellprint samples during a transaction~~.

40. (Original) The method of claim 35, wherein said step of detecting further includes logging each proffered smellprint sample.

41. (Currently Amended) The method of claim 35, wherein said step of detecting further includes at least one of ~~detecting,~~ processing and storing at least one second proffered smellprint sample.

42. (Original) The method of claim 35, wherein said step of detecting further includes using said smellprint sensor to detect at least one of false odorants, man-made smells, abnormal odorants and body heat.

43. (Original) The method of claim 35, wherein said step of verifying includes comparing a proffered smellprint sample with a stored smellprint sample.

44. (Original) The method of claim 43, wherein said step of comparing a proffered smellprint sample with a stored smellprint sample comprises storing, processing and comparing smellprints using at least one of statistical, ANN and neuromorphic techniques.

45. (Original) The method of claim 43, wherein comparing a proffered smellprint sample with a stored smellprint sample includes comparing a proffered smellprint sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

46. (Original) The method of claim 35, wherein said step of verifying includes verifying a proffered smellprint sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

47. (Original) The method of claim 35, wherein said step of verifying includes verifying a proffered smellprint sample using one of a local CPU and a third-party security vendor.